Compartir Archivos de Manera Segura y Autónoma

Escrito por Rafael Bonifaz, Fellow de Fundación Acceso, para taller de la comunidad AutoFormaciónTL.

Cuando se comparten archivos a través de Internet se lo suele hacer a través de un intermediario. Si se utiliza Google Drive, Google se queda con una copia de los archivos; si se comparte con Dropbox, esta empresa se quedará con una copia de los archivos. Gracias a documentos secretos de la Agencia de Seguridad Nacional de Estados Unidos, NSA por sus siglas en inglés, filtrados por Edward Snowden en 2013, se sabe que estas empresas entregan los datos de sus usuarios a la NSA, CIA o FBI si estas agencias se los solicitan sin necesidad de una orden judicial y sin ser notificados.[1]

En este taller se aprenderá a compartir archivos de manera autónoma y segura. La primera parte se verá OnionShare que permite compartir archivos de manera casual y segura a través de Tor. La segunda parte se verá el uso de Nextcloud como servicio cebolla de Tor; en este caso se aprenderá a compartir y tener sincronizadas carpetas para grupos de trabajo. En los dos casos se aprenderá a compartir archivos demanera autónoma y segura sin depender de terceros que podrían copiar nuestros archivos.

1) OnionShare

OnionShare es una aplicación que permite compartir archivos directamente desde una computadora a otra computadora o dispositivos móviles. Para compartir los archivos, María genera un dirección del tipo http://direccion.onion/algun-texto que deberá compartirla solamente a las personas que deben acceder a los archivos. Los únicos requesitos para compartir los archivos es tener instalado Tor y saber la dirección.onion. Estas direcciones son efímeras y se utilizan una sola vez.

OnionShare esta disponible para descarga para Windows, Mac y Linux[2]. En el ejemplo de este taller se utilizará una máquina virtual con Linux Mint 19.1 y otra con Debian 9. En el caso de Linux Mint viene con una versión muy vieja por lo que se recomienda instalar desde los PPA. En el caso de Debian fue necesario activar los repositorios backports. Para Windows y Mac vienen instaladores que deberían funcionar sin problemas y para ver como instalar en otras distribuciones revisar la página web.

1 En el siguiente documento se puede ver una investigación sobre los documentos de Snoden: https://rafael.bonifaz.ec/blog/wp-content/uploads/2017/11/La-NSA-seg%C3%BAn-documentos-de-Snowden-Rafael-Bonifaz-cc.pdf
2 Disponible desde su sitio web https://onionshare.org/

a) Instalar en Debian

Para instalar OnionShare en Debian se debe activar los repositorios backports, para esto se debe editar como root el archivo /etc/apt/sources.list y añadir la siguiente línea

```
deb http://ftp.debian.org/debian stretch-backports main
```

Con esto se activo el repositorio y ahora se lo puede instalar mediante el comando apt:

```
sudo apt update
sudo apt install onionshare
```

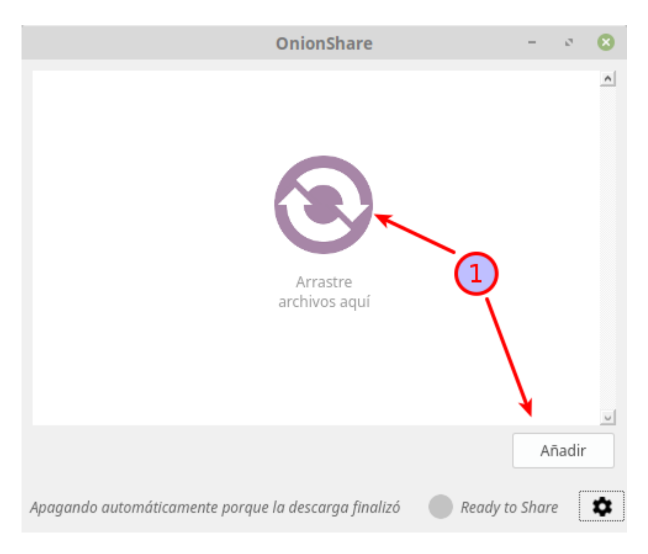
b) Instalar en Linuxmint

OnionShare se puede instalar directamente desde los repositorios de Linuxmint o Ubuntu, pero viene con una versión antigua; por lo que se instalará a través de repositorios PPA:

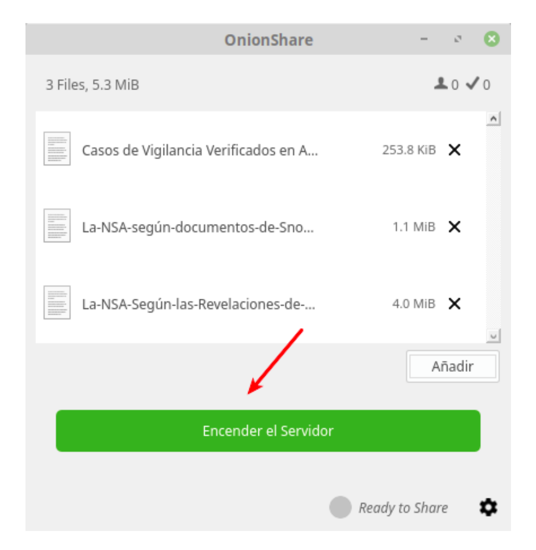
```
sudo add-apt-repository ppa:micahflee/ppa
sudo apt update sudo apt install -y onionshare
```

c) Utilizar Onionshare

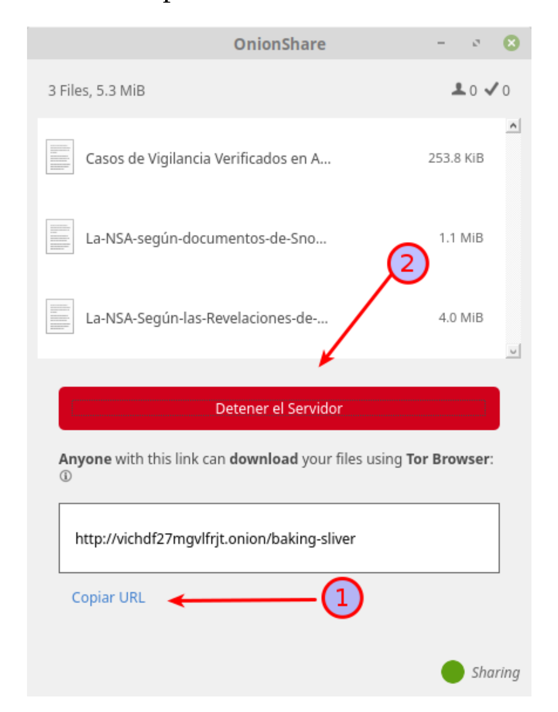
Utilizar Onionshare es bastante simple. Se abre la aplicación, se añaden los archivos ya sea arrastrándolos o buscando desde la aplicación a través del botón añadir como se puede ver en la imagen.



Una vez que se añadieron los archivos se debe hace click en el botón “Encender el Servidor



Una vez hecho esto se espera un rato hasta que se de la opción de “Copiar URL”(1) se active. El enlace que se copia se lo debe compartir a las personas que quieran acceder a los archivos. Si se desea cancelar la compartición de archivos de lo puede hacer con el botón “Detener Servidor”(2).



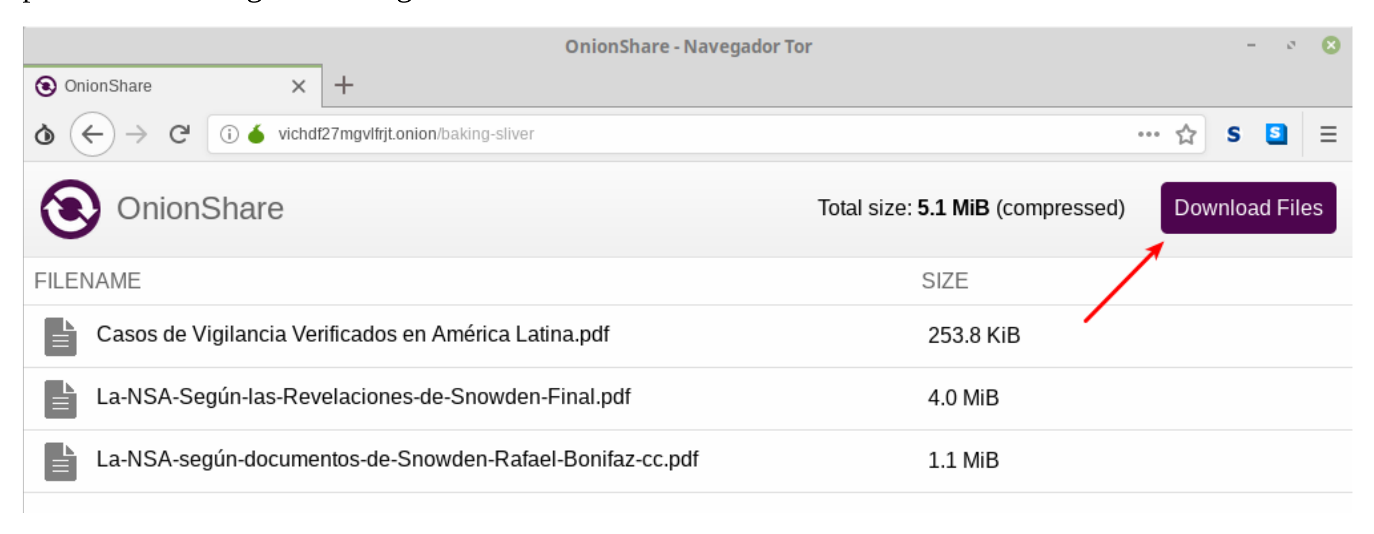
Hay que tomar en cuenta qué:

- Por defecto el archivo se comparte solo a una persona, luego de que la primera persona lo descarga se detiene el servicio. Esta opción se puede cambiar en las configuraciones.
- Los enlaces compartidos son efímeros, si enciende por segunda vez el servidor será un enlace nuevo.

- En las configuraciones de OnionShare se pueden añadir opciones como la de compartir por un tiempo predeterminado, conservar los enlaces, entre otros.

d) Acceder a los archivos

Para acceder a los archivos basta con abrir el enlace compartido en el Navegador Tor como se puede ver en la siguiente imagen:



2) Compartir archivos con Nextcloud

En este ejercicio se harán tres cosas: primero se configurará Apache como un servicio Cebolla de Tor; segundo se instalará Nextcloud en ese servicio; tercero se sincronizarán las carpetas entre computadoras a través de los clientes de NextCloud.

a) Configurar Apache como Servicio Cebolla

Si bien en esta ocasión se configurará Apache como servicio cebolla para instalar Nextcloud, en realidad se podría instalar cualquier aplicación que funcione en un servidor web y escuche en el puerto 80.

Los servicios cebolla tienen ciertas características que vale la pena destacar:

- Proveen anonimato tanto a quién provee el servicio como a quién accede al mismo. Al menos que explícitamente se identifique.
- No se requiere una dirección IP pública para acceder al servicio, pero es necesario poder acceder a través de Tor.
- La comunicación es cifrada entre el servicio oculto y los clientes. Es por esto que se va a implementar solamente el puerto 80 y no el 443. Si se quisiera usar Nextcloud a través de Tor y en la red local habría que usar HTTPS para la red local.
- La dirección .onion no es 100% secreta por lo que es importante proteger las aplicaciones instaladas. Esto mejora en la versión 3 de los servicios ocultos que son relativamente nuevos.

Este laboratorio se realizó utilizando Debian 9 pero funcionará de manera similar en otras distribuciones con Linux.

Lo primero que se hace es instalar Tor y Apache:

```
sudo apt install tor apache2
```

Con esto en el navegador ya es posible acceder a la página a través de la siguiente dirección: http://127.0.0.1.

Ahora se configurará Tor para publicar el servidor Apache como servicio cebolla. Para esto se debe editar el archivo /etc/tor/torrc y configurar las siguientes líneas:

```
HiddenServiceDir /var/lib/tor/nextcloud
HiddenServicePort 80 127.0.0.1:80
```

La primera línea dice el directorio donde se guardará la configuración del el servicio oculto. Este directorio se creará automáticamente luego de reiniciar el servicio Tor. La segunda línea dice que se

publicará como servicio oculto el puerto 80. En este caso estamos publicando un servidor web, pero se podría publicar prácticamente cualquier servicio TCP.

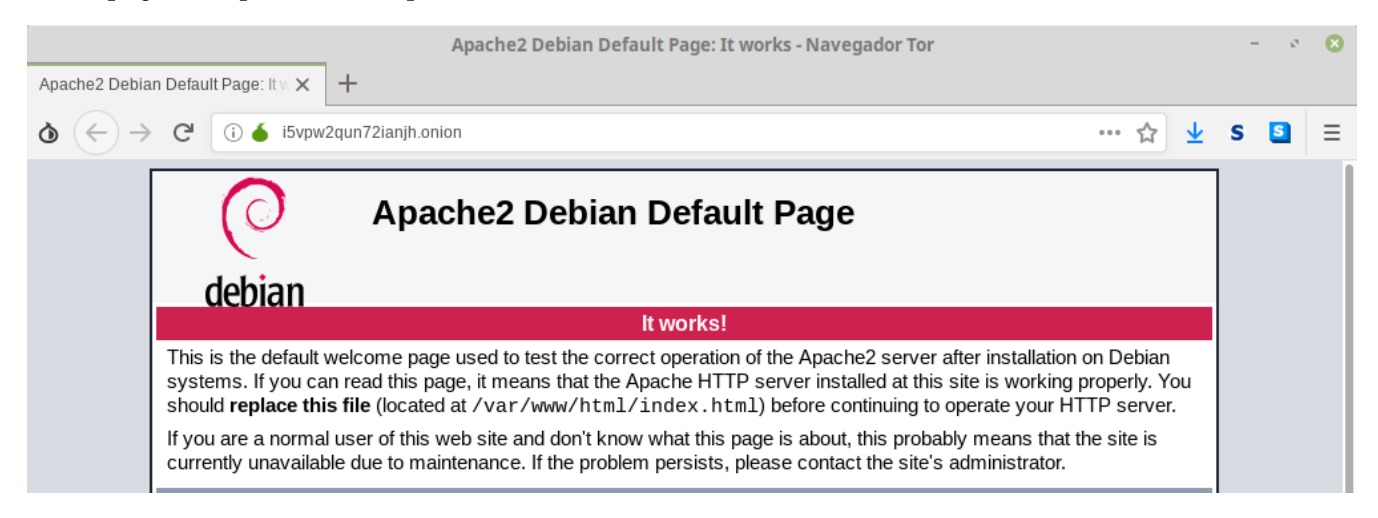
Reiniciar Tor:

```
sudo systemctl restart tor
```

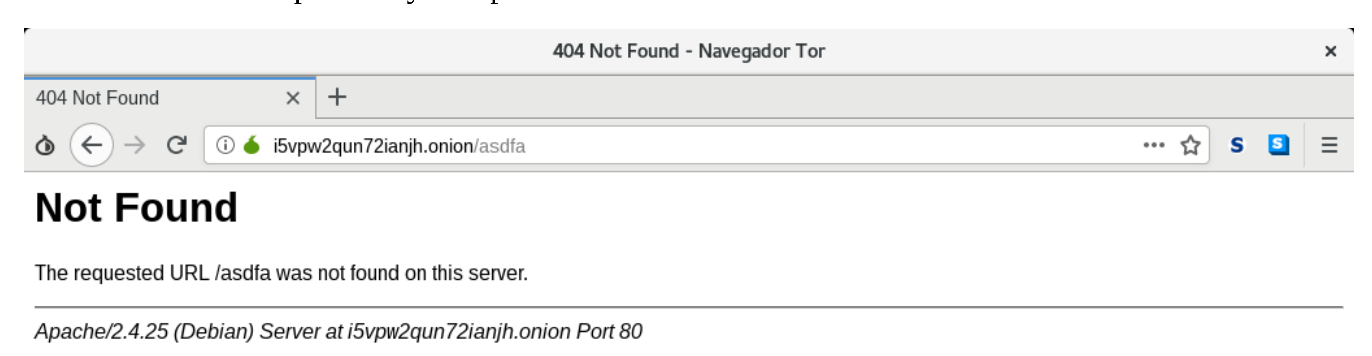
En la carpeta /var/lib/nextcloud se crearán dos archivos: private_key y hostname. El primero guarda tanto la llave pública como la privada del servicio. Este archivo se lo debe cuidar y no se debe compartir. El hostname es la dirección del servicio oculto que es un hash derivado de la llave pública. Para conocer la url del servicio oculto ver el contenido del archivo hostname:

```
sudo cat /var/lib/tor/nube/hostname
i5vpw2qun72ianjh.onion
```

En este caso la url es: i5vpw2qun72ianjh.onion. Al abrir la misma en el navegador Tor se podrá ver la página de pruebas de Apache:



La configuración de Apache por defecto no es segura. Por ejemplo una página de error muestra la versión del sistema operativo y de Apache.



Para realizar un aseguramiento mínimo en Apache conviene editar el archivo /etc/apache2/conf-available/security.conf y modificar las siguientes variables:

```
ServerTokens Prod
ServerSignatures Off
```

Luego se reinicia Apache

```
sudo  systemctl reload apache2
```

Por último se borra el archivo de pruebas de Apache:

```
rm  /var/www/html/index.html
```

b) Instalar Dependencias

Para instalar Nextcloud lo primero que se debe hacer es instalar las dependencias necesarias para que funcione.

```
sudo apt install  mariadb-server libapache2-mod-php apache2
```

En el caso de este ejemplo no es necesario instalar apache2 porque ya fue instalado previamente.

También es importante instalar las dependencias necesarias de PHP. En el caso de Debian son las siguientes:

```
sudo apt install php-gd php-json php-mysql php-curl php-mbstring php-intl php-imagick php-xml php-zip
```

En caso de usar Ubuntu, CentOS u otra distribución recomiendo ver la documentación oficial de Nextcloud[3].

En las pruebas se tuvo problemas con Nextcloud 15 (la versión más nueva la momento de escribir esta guía) al intentar conectar el cliente al servidor. Por este motivo se instaló Nextcloud 14 que funciona muy bien para compartir archivos.

c) Configurar MariaDB

En este ejemplo se esta utilizando la base de datos MariaDB, pero se puede utilizar SqlLite para instalaciones pequeñas o Posgres para instalaciones grandes. Antes de instalar Nextcloud es importante asegurar MariaDB, para esto se ejecuta:

```
mysql_secure_installation
```

Se debe poner clave de root y aceptar las recomendaciones.

Luego hay que ingresar a la consola de configuración de MariaDB para crear la base de datos y el usuario para nextcloud:

```
mysql -u root -p
```

3 Ver instrucciones detalladas acá: https://docs.nextcloud.com/server/14/admin_manual/installation/index.html

Una vez dentro de la consola de MariaDB ejecutar[4]

```
create database nextcloud;
grant all on nextcloud.* to 'nextcloud'@'localhost'
    identified by "ClaveSegura";
```

d) Instalar Nextcloud

Ir a la página de Nextcloud y descargar la última versión disponible de Nextcloud 14[5]. Descargar los archivos ZIP o BZ2 y al menos un hash de verificación.

Por ejemplo se puede descargar el archivo .bz2 y su correspondiente hash de verificación, por ejemplo sha256.

```
$~/Descargas$ sha256sum nextcloud-14.0.6.tar.bz2
1a739b5c4a633d15e68d1db31f785c2e5926b877e165af62f740837077e2f
45f  nextcloud-14.0.6.tar.bz2
$~/Descargas$ cat nextcloud-14.0.6.tar.bz2.sha256
1a739b5c4a633d15e68d1db31f785c2e5926b877e165af62f740837077e2f
45f  nextcloud-14.0.6.tar.bz2
```

Si los códigos coinciden se tiene más seguridad de que se descargó una versión legitima de Nextcloud.

Se descomprime los archivos y se los copia en la dirección /var/www/nextcloud. Luego se hace a apache dueño de la carpeta.

```
tar xvf  nextcloud-14.0.6.tar.bz2
sudo mv nextcloud /var/www/nextcloud
sudo chown -R www-data:www-data nextcloud
```

Antes de instalar es necesario crear un directorio para guardar los datos que debe estar fuera del “DocumentRoot” de apache y se debe poder escribir por el usuario Apache (www-data en Debian y derivados). Por ejemplo se lo puede hacer en la carpeta /var/datos.

```
sudo mkdir /var/datos/
sudo chown -R www-data:www-data /var/datos
```

El último paso previo a ejecutar el instalador de Nextcloud es configurar Apache. En este caso se hará que la aplicación se accesible en http://serviciooculto.onion/nextcloud. Pero se puede configurar de varias formas. Crear el archivo: /etc/apache2/sites-available/nextcloud.conf y añadir el siguiente contenido[6]:

4 Son 2 líneas
5 Este enlace lleva directo a la ubicación de la versión 14 de Nextcloud: https://nextcloud.com/changelog/#latest14
6 Configuración tomada del manual de instalación de Nextcloud.

```
Alias /nextcloud "/var/www/nextcloud/"

<Directory /var/www/nextcloud/>
     Options +FollowSymlinks
     AllowOverride All

     <IfModule mod_dav.c>
          Dav off
     </IfModule>

     SetEnv HOME /var/www/nextcloud
     SetEnv HTTP_HOME /var/www/nextcloud
</Directory>
```

Luego se activa la configuración, se añade el módulo de re-escritura y se recarga el servicio de Apache.

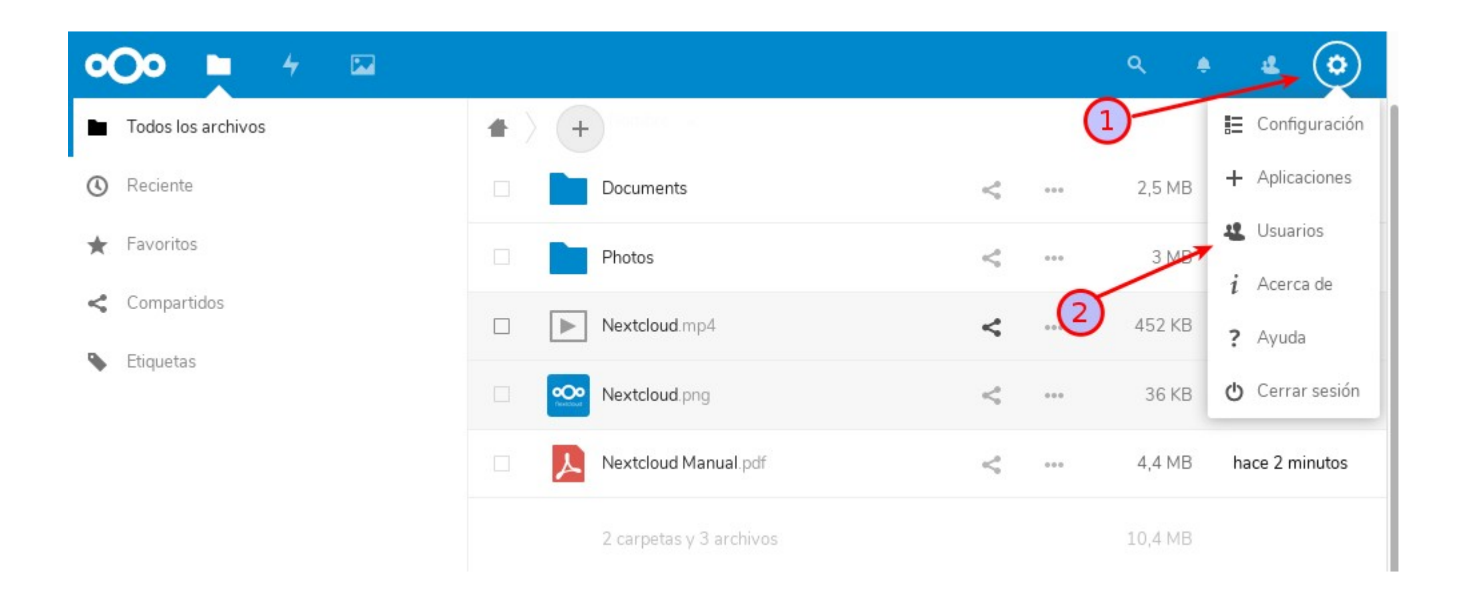
```
sudo a2ensite nextcloud.conf
sudo a2enmod rewrite
sudo  systemctl reload apache2
```

Ahora sí se ingresa a la url por donde se quiere acceder al servicio cebolla y se sigue el asistente de configuración de Nextcloud. En este caso: http://i5vpw2qun72ianjh.onion/nextcloud

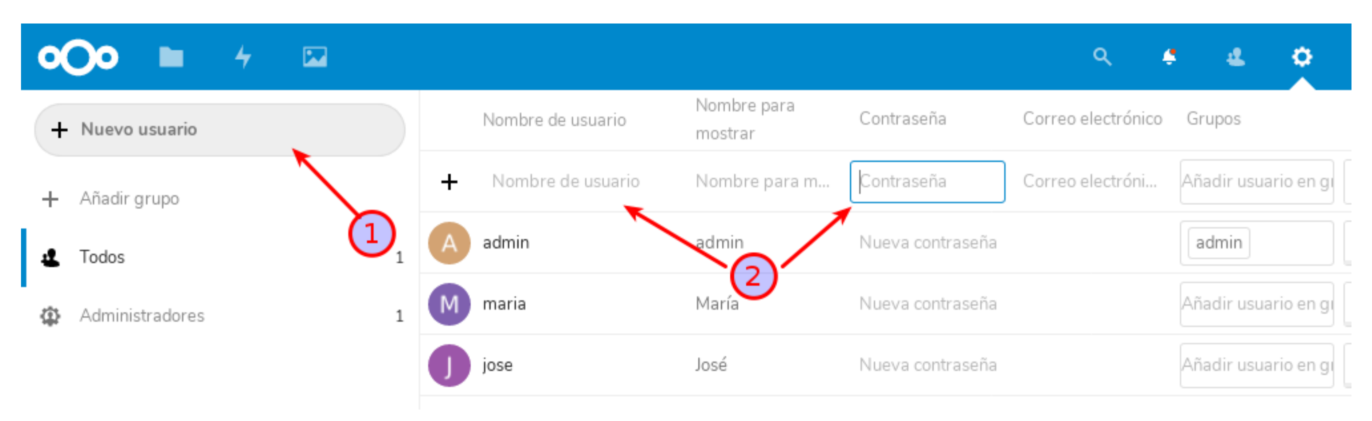


Se crea el usuario administrador que puede tener cualquier nombre, mejor si no se llama admin o administrador. En la carpeta de datos de pone el directorio creado previamente, en este ejemplo /var/datos. En los datos de la base de datos se pone el usuario, la base y la clave creados previamente.

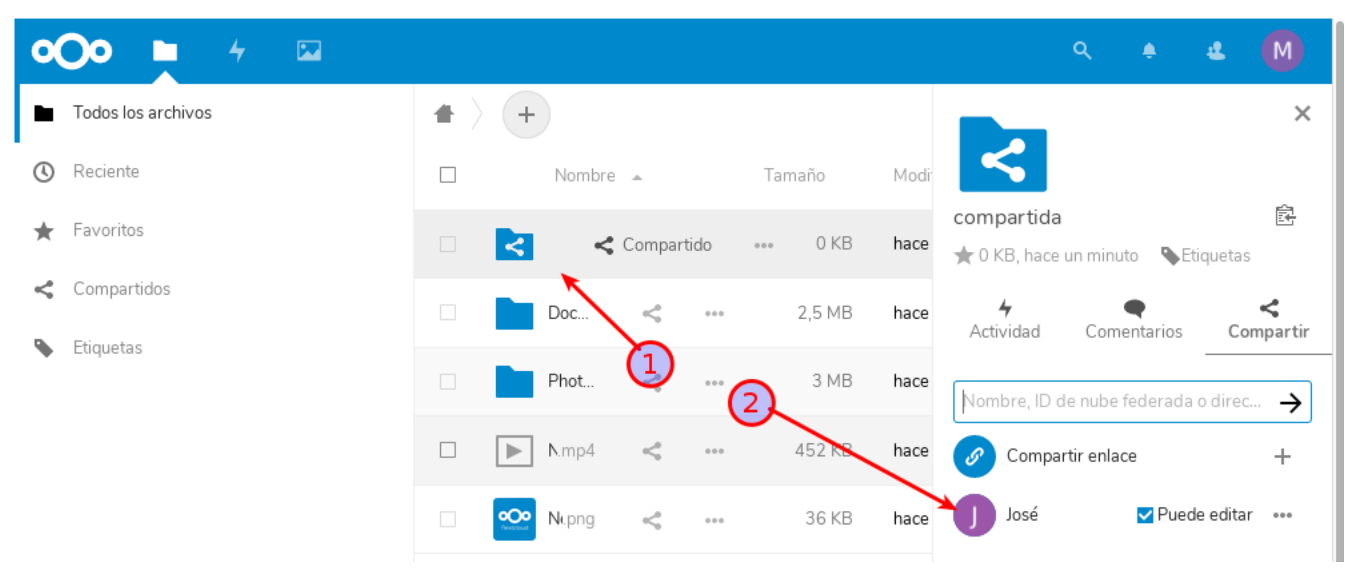
Una vez hecho esto queda instalado Nextcloud y se ingresará a la pantalla de inicio. Ahora se crearán dos usuari@s que compartirán archivos. En este ejemplo l@s usuari@s serán María y José. Para esto se debe hacer click en el ícono de configuración(1) y luego en usuario@(2) como se ve en la siguiente imagen.



En la siguiente pantalla se pone añadir usuario(1) y luego un usuario y una contraseña(2) para cada usuari@ como se ve en la siguiente imagen.



Ahora se puede ingresar al servicio oculto como José o María a través del navegador Tor y compartir archivos. En la siguiente captura de pantalla, María está compartiendo la carpeta “compartida”(1) con el usuario José(2):



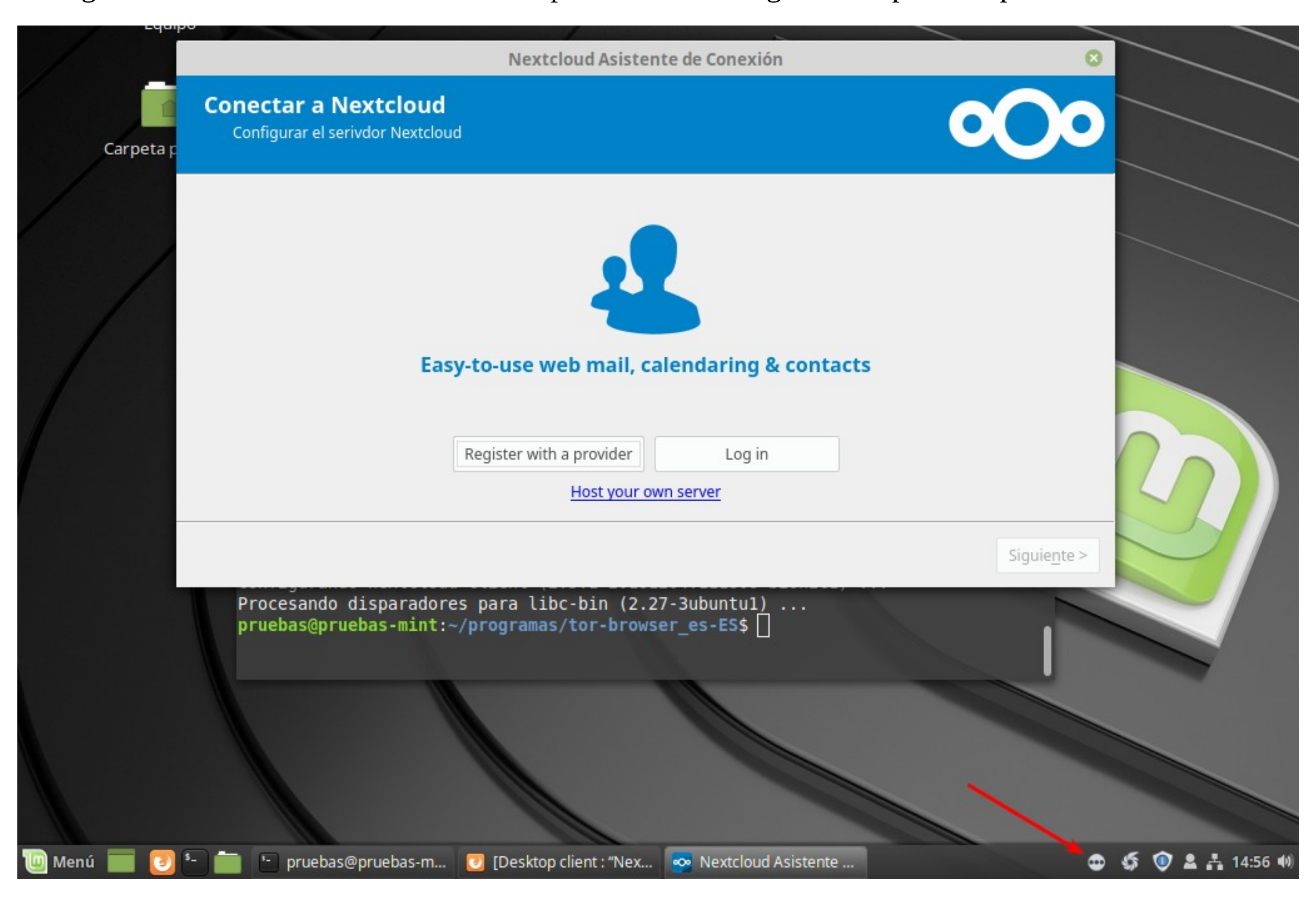
Los archivos compartidos en esa carpeta serán accesibles por José y María.

e) Sincronizar archivos mediante cliente

Hasta ahora se vio como compartir archivos a través del navegador Tor. Esto resulta práctico pero puede ser incómodo. Ahora se verá como hacer para sincronizar los archivos en una carpeta local. Para esto es necesario instalar el cliente de Nextcloud en el equipo, este puede ser Windows, Linux, Mac o Android[7].

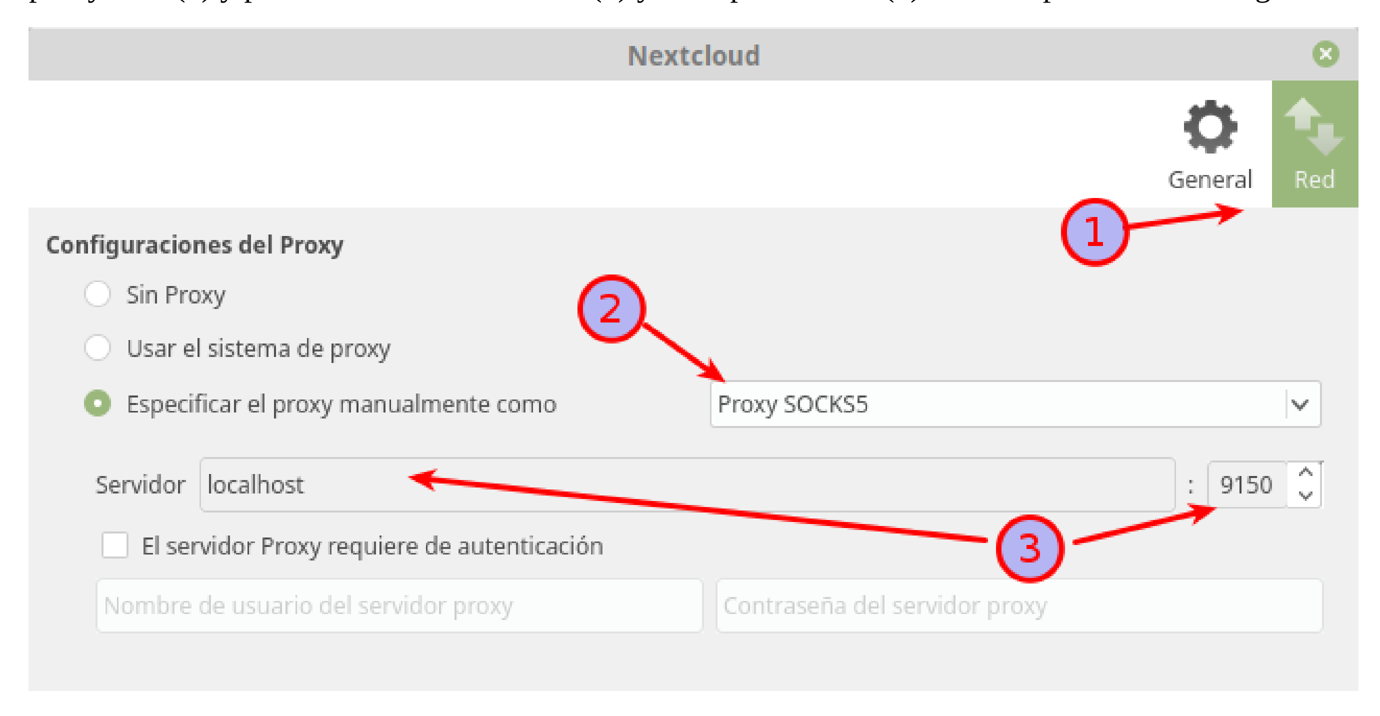
Para la instalación se puede seguir las instrucciones de instalación oficiales de Nextcloud[8]. En el caso de las pruebas se instaló el cliente AppImage en Debian y en el caso de Linux Mint se siguió las instrucciones de configuración del PPA de Ubuntu.

Una vez que se abre el cliente de Nextcloud se inicia un asistente, antes de ingresar al mismo hay que configurar Nextcloud para que utilice Tor. Para esto dependiendo del sistema operativo se debe buscar el ícono de Nextcloud en la barra de estados, hacer click con el botón derecho y acceder a la configuración. En el caso de LinuxMint se puede ver en la siguiente captura de pantalla:

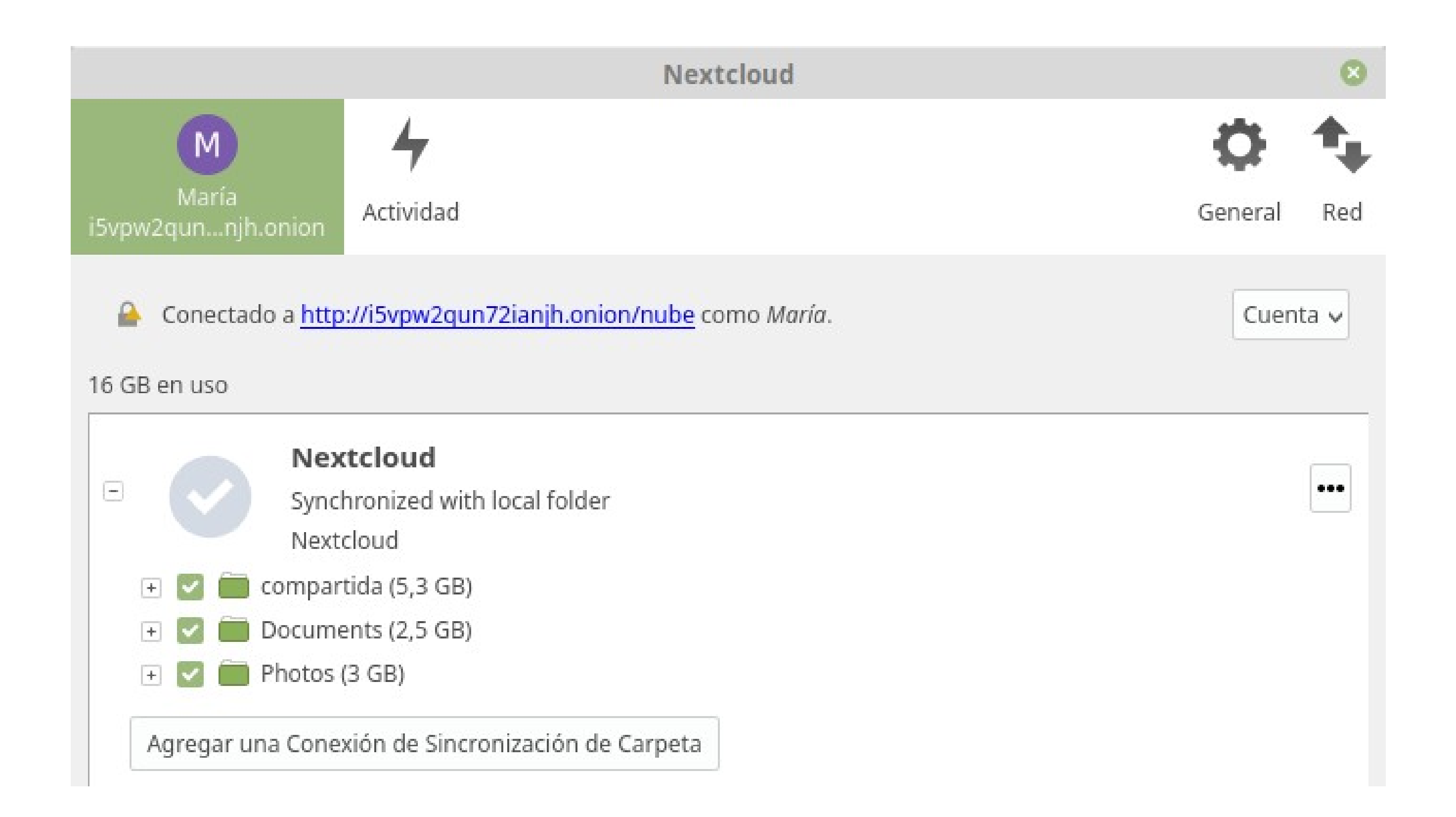


7 En el caso de usar Android a más del cliente de Android se debe utilizar Orbot.
8 Ver instrucciones acá: https://nextcloud.com/install/#install-clients

Esto presentará la configuración de Nextcloud, hacer click en Red(1), luego configurar como proxysocks(2) y poner en servidor localhost(3) y en el puerto 9150(3) como se puede ver la imagen.



Una vez hecho esto se puede seguir con el asistente de configuración de Nextcloud utilizando el url que se uso para ingresar en el navegador Tor y luego acceder con un usuari@ creado previamente (ej. María o José en este ejemplo). **Es importante notar que el navegador Tor debe estar abierto para que esto funcione.** Cuando se terminó el asistente se mostrará una ventana como la siguiente:



Una vez hecho esto se crea una carpeta Nextcloud donde se sincronizan los archivos del servidor. Cuando María copie los archivos en esa carpeta, los mismos se subirán al servidor de Nextcloud automáticamente si el cliente esta ejecutándose. Si María tiene el cliente ejecutándose en otra computadora o en el celular podrá acceder a los archivos de manera automática. Los archivos copiados en la carpeta “compartida” son accesibles tanto por María y José.

En el caso de sistemas Linux se puede configurar el cliente para que funcione sin la necesidad de tener el navegador Tor abierto. Para esto se debe instalar el paquete tor y configurar el puerto como 9050 en lugar de 9150.

```
sudo apt install tor
```